

**Technická univerzita v Liberci**

**Ekonomická fakulta**

Studijní program: B 6209 Systémové inženýrství a informatika

Studijní obor: Podnikatelská informatika

**Návrh ochrany dat uživatele**

Concept of user's data protection

Číslo závěrečné práce

BP – EF – KIN – 2010 – 04

Ivana Kallmünzerová

Vedoucí práce: Ing. Zbyněk Hubínka, Katedra Informatiky

Konzultant: Mgr. Tomáš Žižka, Katedra Informatiky

Počet stran: 31

Počet příloh: 0

Datum odevzdání: 7.5.2010

## Prohlášení

---

Byla jsem seznámena s tím, že na mou bakalářskou práci se plně vztahuje zákon č.121/2000 Sb. o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědoma povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladu, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracovala samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

V Liberci, 05. 05. 2010

---

## **Anotace**

---

Tématem této bakalářské práce je návrh ochrany uživatelských dat. Teoretický základ práce se zabývá především riziky poškození uživatelských dat, popisem datových nosičů – hardwarem, který se používá k ukládání či přenášení dat a zhodnocením výhod a nevýhod těchto jednotlivých datových nosičů. Praktická část je potom zaměřena zejména na možnosti zálohování a srovnání parametrů jednotlivých metod zálohování dat. Po zhodnocení a výběru nejvhodnějšího hardwaru pro zálohu dat jsou v práci obsaženy čtyři testy různých způsobů vytváření záloh. Testovány byly tyto možnosti: manuální kopírování pomocí souborového manažera, zálohování dat pomocí Windows, využití programu Create Synchronicity a využití programu AASync. Cílem celé práce je najít vhodný program ve formě freeware umožňující vytvořit zálohu v rychlejším čase, než jakého je dosaženo pomocí kopírování souborů za využití souborového manažera.

## *Klíčová slova*

---

Záloha dat

Datová média

Poškození dat

## **Abstract**

---

Topic of this bachelor work is Concept of user's data protection. The theoretical part is about threads that can damage user's data and about data storages – a hardware used for saving and transporting data. The practical part is about backups possibilities. After choosing most suitable data storage were run four tests of making data backups. These tests were copying data with file manager, Windows backup, Create Synchronicity and AASync. Main goal of this work is to found at least one freeware that can make backup more quickly than manual copying data to the storage with file manager.

## *Keywords*

---

Data backup

Data storage

Damage of the data

## Obsah

---

<b>PROHLÁŠENÍ .....</b>	<b>2</b>
<b>ANOTACE.....</b>	<b>3</b>
KLÍČOVÁ SLOVA .....	3
<b>ABSTRACT .....</b>	<b>4</b>
KEYWORDS .....	4
<b>OBSAH.....</b>	<b>5</b>
<b>SEZNAM ZKRATEK.....</b>	<b>6</b>
<b>SEZNAM OBRÁZKŮ .....</b>	<b>7</b>
<b>ÚVOD.....</b>	<b>8</b>
<b>NOSNÁ MÉDIA DAT.....</b>	<b>9</b>
PEVNÉ DISKY.....	9
DISKETY – FLOPPYDISKY .....	13
OPTICKÉ NOSIČE - CD A DVD.....	15
PAMĚTI TYPU FLASH .....	17
<b>POŠKOZENÍ DAT .....</b>	<b>19</b>
POŠKOZENÍ HARDWARE .....	19
SOFTWAREOVÁ RIZIKA.....	21
<b>ZPŮSOB PRO ZNOVUZÍSKÁNÍ ZTRACENÝCH DAT.....</b>	<b>25</b>
<b>ZÁLOHOVÁNÍ.....</b>	<b>27</b>
VOLBA MÉDIA .....	27
KOPÍROVÁNÍ SOUBORŮ .....	27
WINDOWS ZÁLOHOVÁNÍ .....	29
CREATE SYNCHRONICITY .....	31
AASYNC .....	33
<b>ZÁVĚR.....</b>	<b>36</b>
<b>LITERATURA .....</b>	<b>39</b>
CITACE.....	39
BIBLIOGRAFIE .....	39

## Seznam zkratek

---

AND – architektura hardwarové stavby disku flash

ARLL – Advanced Run Length Limited, , způsob zápisu na magnetická média

ATA – advanced technology attachment, typ fyzického připojení disku do počítače

CD – compact disc, optický nosič

DINOR – architektura hardwarové stavby disku flash

DVD – digital versatile disc, optický nosič

EEC – Error Correction Code, opravný kód v nejnižší úrovni formátu pevného disku

FAT – File Allocation System, způsob ukládání dat na pevný disk

FM – Frequency Modulation, způsob zápisu na magnetická média

HW – hardware, fyzická část informačních technologií

CHKDSK – Checkdisk, program na opravu chyb v logické tabulce pevného disku

IDE – standard připojení zařízení na uchovávání dat

IT – informační technologie

MFM – Modified Frequency Modulation, způsob zápisu na magnetická média

NAND – architektura hardwarové stavby disku flash

NOR – architektura hardwarové stavby disku flash

NTFS – New Technology File System, způsob ukládání dat na pevný disk

OS – operační systém

RAM – random Access memory, typ paměti na bázi technologie flash

RLL – Run Length Limited, , způsob zápisu na magnetická média

SATA – seriál ATA, typ fyzického připojení disku do počítače

SD – Secure Digital, paměťová karta na základě technologie flash

SW – software, programové vybavení

XD – extreme digital, paměťová karta na základě technologie flash

## Seznam obrázků

---

Obr. 1 - Licence programu Total Commander .....	28
Obr. 2 - Total Commander - přepis souboru .....	28
Obr. 3 - Výběr knihoven zálohy Windows .....	29
Obr. 4 - Průběh zálohování ve Windows .....	30
Obr. 5 - Vytvoření profilu v Create Synchronicity .....	31
Obr. 6 - Create Synchronicity, průběh zálohování .....	32
Obr. 7 - AASync - vytvoření profilu .....	34

## Úvod

---

Téma mé bakalářské práce je návrh ochrany uživatelských dat. Toto téma je mi velice blízké, protože jsem sama několikrát o svá data přišla. Dalším důvodem proč jsem zvolila téma ochrany uživatelských dat je mé působení ve firmě Liberecká IS, a.s. na pozici pracovníka oddělení podpory uživatelů. Základní činností, kterou zde vykonávám je řešení uživatelských problémů s počítači. Tyto problémy jsou různě závažné, některé lze řešit malým zásahem pomocí vzdáleného přístupu na uživatelském počítači, jiné je nutné řešit zásahem přímo na pracovišti uživatele. Bohužel poměrně častým řešením je celková reinstalace operačního systému a dalších používaných aplikací. Přestože většina uživatelských dat je umístěna na serveru s vlastním zálohováním, mají uživatelé v počítačích důležitá data uložená na místním disku. Ne vždy se jedná o osobní data, nebo pracovní data stažené ze serveru. Na místním disku bývají uloženy licenční klíče a certifikáty k odborným programům. Taková data je potřeba z disku dostat dříve než se začne s reinstalací operačního systému. Nahrazení licencí a certifikátů je komplikovaný a zdouhavý proces. Zde se dostáváme k hlavnímu tématu mé práce a to k zálohování dat běžně dostupnými prostředky. V praxi je potřeba provést zálohu co nejrychleji, aby se počítač po reinstalaci dostal zpět ke svému uživateli co nejdříve.

Cílem této práce je najít nejrychlejší cestu zálohy dat bez použití placeného software. Jedinou výjimkou bude software zabudovaný přímo v systému Windows, který ač je placený, je dostupný většině uživatelů. Jako úspěch budu považovat pokud se mi podaří nalézt freeware který vytvoří bez problémů zálohu za minimálně stejný čas jako ten který bude dosažen při kopírování testovacího objemu dat.

První kapitola pojednává o typech běžných nosných datových nosičích. Zpracování této teoretické části mi přineslo důležité poznatky o vhodnosti použití různých typů médií pro provedení zálohy. Druhá kapitola je především o možnostech poškození dat. Zde jsem vybrala takové způsoby poškození dat či datových médií se kterými jsem se setkala buď během praxe nebo svého osobního života. Ve třetí kapitole jsou zmíněny některé způsoby získání ztracených dat. Ve čtvrté a páté kapitole bude popsáno zálohování dat pomocí freewareových zálohovacích systémů. V závěru zhodnotím nejlepší způsob zálohování a zda se mi podařilo dosáhnout svého cíle.



## Nosná média dat

---

V současné době používáme některé druhy nosných médií častěji než ostatní, což je dáno především jejich kapacitou a finanční dostupností pro většinu uživatelů. V této části mé práce se budu věnovat nejčastěji používaným nosičům dat. To znamená, že níže nebude pojednáno o velice starých metodách záznamů dat (jako byly děrné štítky a pásky) a také o úzce specializovaných a velice drahých systémech jako jsou páskové zálohy serverů.

### *Pevné disky*

---

Pevný disk neboli anglicky „hard disk“ je neodmyslitelnou součástí dnešních osobních počítačů. Jedná se o magneticky zapisovatelné médium pro uložení dat. Název pevný disk je odvozen od pevných hliníkových kotoučů, které nesou zapsaná data. První pevný disk vyrobený společností IBM měl kapacitu celých 5 MB a jeho velikost poněkud připomínala šatní skříň. Další typ disku, už o mnoho menší co do fyzické velikosti, měl kapacitu 10 MB. Současný trend spočívá v neustálém zvětšování kapacity disku a zároveň ve zmenšování jejich fyzické velikosti.

Pevné disky lze v zásadě rozdělit do kategorií podle rozhraní, přes které komunikují s ostatními elektronickými komponentami počítače. U osobních počítačů jsou nejčastěji použita rozhraní ATA a SATA, přičemž je zřejmé, že SATA disky začínají nahrazovat starší disky typu ATA. Další možné kritérium pro rozdělení disků představuje jejich velikost. Na trhu jsou k dostání především disky o velikosti 2,5" a 3,5". Menší 2,5" disky nacházejí své využití v noteboocích a 3,5" disky jsou používány převážně ve stolních počítačích. Pevné disky se také vyskytují ve formě externích neboli přenosných disků. Takové disky jsou většinou zabudovány v plastové schránce a k počítači se připojují buď přes rozhraní USB, nebo FireWire. Zásadní rozdíl pro uživatele externích disků představuje způsob napájení těchto zařízení. Některé disky jsou napájené pouze z datové zásuvky ze zdroje počítače. Takové disky jsou vhodné zvláště pro ty uživatele, kteří potřebují od disku vysokou mobilitu, neboť tyto disky mají často menší velikost (1,8" a 2,5"). Větší disky jsou v externím provedení často vyráběny s vlastním napájením, tj. že se musí připojit ke zdroji napětí 230 V, což znamená, že tyto disky bývají méně mobilní, ale na druhou stranu se dají lépe použít jako rozšíření kapacity paměti počítače, protože nevytěžují zdroj.

Konstrukčně jsou si různé pevné disky velice podobné, hlavní rozdíly lze v podstatě nalézt ve velikosti a způsobu provedení jednotlivých komponent. Vnější část pevného disku tvoří kovový kryt, jenž chrání jeho citlivé vnitřní části. Uvnitř disku najdeme několik hliníkových kotoučů – ploten. Plotny jsou pokryté malou vrstvou magneticky měkkého materiálu, na kterou se zaznamenávají data. Plotny jsou nasazeny na válcový šroub, který je poháněn elektromotorem. Zaměříme-li se na rychlost ploten, můžeme shrnout, že v případě 3,5" disku se setkáváme nejběžněji s rychlostí ploten 7 200 otáček za minutu menších 2,5" disků činí rychlost ploten 5 400 otáček za minutu. Existují i disky s vyšší nebo nižší rychlostí otáček – tyto typy vznikly na základě různých provozních požadavků, mezi něž patří například hlučnost. Každá plotna standardně zahrnuje dvě čtecí/zapisovací hlavy – z každé strany jedna (existují výjimky – u starších jednoplotnových disků byla magnetická vrstva jen na jedné straně, tudíž i jen jedna čtecí/zapisovací hlava). Samotná hlava se vznáší nad povrchem ploten ve vzdálenosti, která řádově činí několik mikrometrů. Každá hlava má svůj vystavovací mechanismus, který ji na principu elektromagnetu umísťuje nad povrch disku do potřebné vzdálenosti pro čtení nebo zapsání dat. Protože pevný disk obsahuje pohyblivé části, stává se náchylným na mechanické poškození. Aby se uživatel vyhnul mechanickému poškození, je třeba dbát na stabilitu disku. I při malých, ale častých otřesech může dojít k narušení struktury ploten. Vedle mechanického poškození disku často hrozí i poškození zápisu dat vlivem působení magnetické síly. Z tohoto důvodu není vhodné vystavovat pevné disky magnetickým polím. Některé disky, jež jsou součástí modernějších notebooků, jsou vybaveny tzv. akcelometrem, který v okamžiku prudkého vnějšího zrychlení zapnutého disku (například při pádu) odtáhne čtecí/zapisovací hlavy mimo plotny tak, aby došlo k zamezení porušení povrchu disku, neboť disk s poškozeným povrchem se stává v daném místě nečitelným. Proto je také nesmysl otevírat funkční pevný disk. Jakmile se na plotny dostane prach, není možné je přečíst, tudíž veškeré disky zbavené vnějšího pláště jsou navždy nefunkční.

Disk jako nosné médium není „nesmrtelný“ – svou konstrukcí a fyzikální podstatou se postupně opotřebovává. Toto opotřebování je dáno v první řadě teplotou, která vzniká při práci disku. Důsledkem neustálého přehřívání disku je jeho postupné poškozování. Jedním z prvních příznaků poškození disku je vyšší chybovost při práci s daty. Další symptomy, které se postupně začínou projevovat, jsou neobvyklé zvuky linoucí se z disku při práci. Různé škrábavé a klapavé zvuky mohou být způsobeny různou teplotní roztažností materiálů použitých v disku. V extrémních případech často dochází k zaseknutí disku – plotny se

nemohou z důvodu tření pohybovat. Proto je důležité, aby pevné disky měly správné podmínky pro jejich bezchybnou práci, to znamená dostatečné chlazení<sup>1</sup>. V zásadě platí, že při instalaci pevného disku do počítače je nutné, aby kolem disku bylo umožněno proudění vzduchu, nebo aby měl disk vlastní chladicí soustavu, a to buď aktivní (větráček), anebo pasivní (speciální chladicí sloty). Některé externí disky, zejména ty s vlastním napájením ze zdroje 230 V, mají aktivní chladicí soustavu.

Jak uvádí ve své publikaci Dembowski magnetický záznam dat funguje na principu magnetické hystereze<sup>2</sup>. Pro zápis dat je třeba vytvořit systém, který zaznamená jednotlivé „0“ a „1“ na povrch disku. K tomuto účelu existuje několik metod, díky nimž se určí, kde začínají a končí jednotlivé bity. Nejstarší metodou je Frequence Modulation (FM), která funguje na principu změny magnetického toku. Aby došlo k oddělení jednotlivých bitů (jedniček a nul), je před každým datovým bitem vyslán synchronizační impuls. Proto je pro zapsání jedničky nutné změnit velikost magnetického toku dvakrát, kdežto u nuly je potřebná pouze jedna změna. Tento princip s sebou nese jeden veliký zápor, a to skutečnost, že mnoho místa na povrchu disku je zabráno právě těmito synchronizačními impulzy, tudíž je následně omezeno místo pro zápis samotných dat. Novější je metoda MFM (Modified Frequence Modulation), která předpokládá konstantní rychlost otáčení disku. Frekvenční signál se tak zaznamenává společně s datovým signálem. Pro každý bit je dána stejně velká oblast a pro zápis jedničky je změna magnetického toku provedena uprostřed této oblasti. U nuly, která nenásleduje po jedničce, je změna magnetického toku provedena na začátku oblasti. Tímto způsobem je možné zaznamenat až o 100% více dat než metodou FM. V současnosti se ale primárně používají metody RLL (Run Length Limited) a ARLL (Advanced Run Length Limited). Tyto metody spočívají v překódování dat. Skupiny bitů se převádí do kódu s proměnnou délkou kódu. V praxi to znamená, že mezi dvěma jedničkami je zapsán proměnlivý počet nul. Metoda RLL vkládá mezi jedničky až sedm nul. Metoda ARLL vkládá mezi jedničky tři až devět nul. Tyto metody umožňují rychlejší zápis dat a vyšší hustotu zápisu. Oproti metodě MFM je kapacita větší až o 50% při použití metody RLL a až o 100% větší při použití metody ARLL. Metody pro zápis dat na pevný disk se neustále zlepšují a zrychlují, díky tomu jsou

---

<sup>1</sup> Optimální provozní teplota pevného disku se pohybuje okolo 35 - 45°C.

<sup>2</sup> [2]"Ve fyzice je hystereze označení skutečnosti, že stav systému závisí na stavech předchozích a historii vstupů. Graf průběhu fyzikálních změn při cyklickém opakování podmínek se nazývá hysterezní křivka, příkladem může být závislost magnetické indukce látky, která je jádrem cívky, na intenzitě magnetického pole této cívky, kdy se projeví magnetická polarizace."

vyvíjeny rychlejší a objemnější disky. Nové způsoby zápisu jsou odvozeny od metod RLL a ARLL. [1, s. 164 - 167]

Data na pevném disku se zapisují do soustředných kružnic neboli stop. Jednotlivé stopy umístěné nad sebou na jednotlivých plotnách tvoří cylindr. Při zaplňování disku se nezaplňují postupně jednotlivé povrchy ploten, ale data jsou obsazována postupně do jednotlivých cylindrů. Tímto dochází ke zvyšování rychlosti práce s diskem, protože rameno čtecí/zapisovací hlavy se nemusí pohybovat v tak velkém rozsahu. Datová struktura disku (v rámci jednotlivých ploten) je rozdělena do stop a sektorů. Disk lze rozdělit i do diskových oddílů, kde každý oddíl v operačním systému vystupuje jako samostatný disk. Toto rozdělení mělo smysl u starších OS; například Windows 98 uměly pracovat pouze se systémovým diskem o maximální kapacitě 4 GB. Nové systémy mohou pracovat s libovolně velkým systémovým diskem. V některých případech je dokonce nevhodné disk takto dělit. Ve své praxi jsem se setkala s případy, kde takovéto rozdělení disku způsobilo pád vlastního systému z důvodu nedostatku místa pro práci vlastního OS.

Pro přístup k datům se používá několik systémů formátování disků. Úplně první formátování disku je provedeno již při výrobě. Jedná se o nízkoúrovňové formátování, jež softwarově vyřadí chybné oblasti disku. Tím se docílí zvýšení spolehlivosti disku z hlediska eliminace poškození dat. Součástí nízkoúrovňového formátování je i opravný kód EEC (Error Correction Code), jenž je schopen data z chybného sektoru (jsou-li čitelná) přesunout do vedlejšího sektoru a chybný sektor je zapsán v logické tabulce jako nefunkční. Uživatel může nízkoúrovňové naformátovat disk několika způsoby. V některých (především starších) OS je možnost nízkoúrovňového formátování přístupná ze systému BIOS. Druhou z variant tohoto formátování představuje speciální SW. Nebezpečí tohoto postupu tkví v tom, že se z logické tabulky smažou veškeré informace o chybných sektorech a disk začne být nespolehlivý pro ukládání dat. Jedinou výjimkou, kdy by se k nízkoúrovňovému formátování mělo přistoupit, je napadení disku velmi agresivními viry, které jiným způsobem nejdou odstranit.

Další typy formátování disků slouží k určení způsobu ukládání dat. Nejčastěji používané systémy jsou v podstatě dva (od nich se odvozují některé další varianty), a to starší systém FAT (File Allocation Table) a NTFS (New Technology File System). Systém FAT je starší je však stále nachází své využití například u herních konzol.

Systém FAT ukládá systém data do takzvaných „clusterů“. Cluster lze jednoduše popsat jako logicky spojené sousedící sektory. Jednotlivé sektory mají velikost 512 bajtů. Systém FAT pracuje s 16bitovým adresováním. Proto je maximální počet sektorů, který je možno spravovat 65 536. Díky tomuto systému je možné spravovat diskové oddíly o velikosti nejvýše 2 GB. Data se postupně ukládají do za sebou jdoucích clusterů. Jak se s daty pracuje v průběhu času, dochází k vymazávání, čímž se uvolňují různé cluster. Při dalším zápisu se data ukládají do volných clusterů vzniklých vymazáváním a není-li dost místa pro uložení do po sobě jdoucích clusterů, datový soubor se rozdělí. Tímto způsobem se prodlužuje čas nutný pro přístup k datům, protože čtecí/zapisovací hlavy musí „skákat“ mezi jednotlivými, často vzdálenými clustery. Ke zrychlení práce disku, se kterým se nějakou dobu pracovalo, slouží nástroj defragmentace disku. Tento nástroj spustí kontrolu disku a přeskupí obsah jednotlivých clusterů tak, aby data v nich uložená na sebe logicky navazovala.

Novější systém NTFS je výkonnější. Hlavní změny oproti systému FAT se týkají vyšší spolehlivosti. Každá změna v systému souborů se zapisuje do souboru protokolu, který zaznamenává všechny údaje o správně vykonaných transakcích. Při vzniku chyby se po restartu systému spustí kontrola systému souborů (CHKDSK) a pokud je to možné, opraví se nekonzistentní data. Pokud oprava není možná, poškozená data se nenačtou vůbec. NTFS ukládá data do clusterů podobným způsobem jako systém FAT, ale s tím rozdílem, že díky 64bitovému adresování může být nejvyšší kapacita disku 17 miliard GB.

### *Diskety – Floppydisky*

---

Diskety jsou v současné době považovány za již zastaralou technologii pro přenášení a ukládání dat, ale i přes jejich stáří se i dnes pro ně najde využití. V neposlední řadě z toho důvodu, že v nedávné době (cca 5 – 10 let nazpět) byly nejrozšířenějším médiem pro přenášení dat mezi jednotlivými zařízeními. Disketová mechanika bývala zcela běžnou komponentou osobních počítačů i prvních notebooků. V současné době se disketové jednotky do počítačů standardně nemontují, přesto je stále na většině základních desek integrována 34pinová zásuvka pro datový kabel. U kabeláže zdrojů napětí jsou stále k nalezení malé konektory k připojení disketové mechaniky. Tyto hardwarové součásti jsou v současných počítačích instalovány zejména kvůli speciálnímu postavení disketových mechanik v systémech. Díky nim lze nastartovat OS i po vážnější chybě. Z diskety je možné spouštět

méně náročné operační systémy, zejména systém DOS či některé distribuce OS Linux. Disketová mechanika se dá považovat za záchranný pás počítačového systému, protože právě z disket lze obnovit některá systémová nastavení, jako jsou ovladače ATA a SATA. U nových počítačů již není disketová mechanika běžnou součástí HW soustavy, ale připojit externí mechaniku přes rozhraní USB není problém. Taková mechanika na úrovni BIOSu poté zaujímá postavení klasické mechaniky.

Jako záznamové médium pro ukládání dat slouží v disketách umělohmotný kotouč pokrytý magnetickou vrstvou tzv. floppy. Zápis a uchování dat fungují na principu magnetické hystereze. To znamená, že magnetický materiál si uchová hodnoty síly magnetického pole i po ukončení jeho působení. Tento jev je dán změnou prostorové orientace magnetických dipólů. Data se tímto způsobem zaznamenávají do soustředných kružnic, takzvaných stop. Jednotlivé stopy jsou pak rozděleny do sektorů. Kapacita média je dána hustotou stop, tj. jejich vzdáleností. U nejčastěji používaného typu disket je tato vzdálenost 0,115 mm, což umožňuje médiu zaznamenat až 1,44 MB. Velikost sektorů je dána především formátováním. Například velikost sektoru OS MS-DOS činí 512 bajtů.

Samotné nosné medium – diskety prošly několika vývojovými kroky. Stěžejním důvodem těchto změn bylo navýšení kapacity a mj. rovněž lepší možnost ochrany před mechanickým poškozením. Floppy disk je velmi citlivý na změny magnetického pole, působením i slabého magnetického pole je možné uložená data nevratně poškodit. Avšak data na disketách mohou být poškozena nejen působením magnetického pole, ale, floppy je stejně tak citlivý na prach či otisky prstů na kotouči. Takovéto mechanické bariéry znemožní číst uložená data. Dalším nebezpečím je také zalomení disku, při kterém se také nenávratně poškodí.

První diskety o velikosti 5,25" a maximální kapacitě 720 KB byly náchylné k mechanickému poškození. Plastový obal byl velmi ohebný a otvory sloužící k přístupu k datům nebyly nijak chráněny. Kulatý otvor uprostřed pětipalcového disku, určený pro vodící motorek mechaniky byl sice u některých značek zesílený, ale i tak docházelo ke značnému opotřebení při používání. Další často poškozovanou částí disku je takzvaný indexový otvor, který slouží k nastavení disku do nulové pozice – tj. na začátek stopy. Neméně důležitým prvkem na tomto typu disket je zářez na okraji plastového obalu. Slouží jako ochrana proti zápisu. Přelepením tohoto otvoru neprůhledným materiálem je disketa uzamčena proti zápisu.

Novější typ disket má rozměr 3,5" a maximální kapacitu o velikosti 1, 44 MB. Oproti výše popsanému typu disket je konstrukčně odolnější, neboť má daleko pevnější plastový obal, takže nehrozí tak velké riziko mechanického poškození. Otvory pro čtení a indexaci disku jsou skryté pod kovovým krytem, který se odsune až po vložení disku do mechaniky. Dále byl přidán kovový vodící kroužek do středu floppy, který umožňuje daleko spolehlivější uchycení hnacího motoru mechaniky. Ochrana proti zápisu je tvořena opět otvorem v těle disku, ale s tím rozdílem, že se zakrývá pomocí plastového čtverečku, který je taktéž součástí diskety. Ovšem princip ochrany proti zápisu je přesně opačný než u staršího typu disket. Ochrana je odstraněna v případě zakrytého otvoru. Jeho otevřením disketu ochráníme proti přepisu uložených dat, či zápisu nových.

### *Optické nosiče - CD a DVD*

---

V současnosti jsou jedním z nejrozšířenějších způsobů přenosu dat mezi osobními počítači optické nosiče. Jako první se objevily kompaktní disky (CD) coby nosiče hudby. V dnešní době si asi již nedokážeme představit osobní počítač či notebook bez mechaniky CD/DVD. Zřejmě jedinou výjimku tvoří malé notebooky, do nichž se tento typ mechaniky nevejde.

Jednotky CD a DVD se dají k počítači připojit několika způsoby. Nejstarší způsob je přes IDE rozhraní. Novější typy jdou připojit přes rozhraní SATA nebo přes USB port – toto řešení se používá především u externích mechanik.

Disky CD a DVD používají podobný princip záznamu dat. Mechaniky a vypalovačky DVD jsou kompatibilní pro použití s CD. Opačně kompatibilita neplatí. Samotný princip čtení dat je založen na odrazení laserového paprsku od nerovného povrchu disku CD nebo DVD. Aby bylo možné odrážet laserový paprsek, jsou disky CD a DVD vyrobeny z několika vrstev různých materiálů. Základní tělo nosiče, v němž jsou vylisovány (nebo vypalovány u jiného typu disku) píče a landy<sup>1</sup>, nesoucí informaci je tvořeno průhlednou umělou hmotou (nejčastěji polykarbonátem). Další vrstvou je tenká hliníková fólie, jež umožňuje čtení dat z disku pomocí laseru. Na reflexní vrstvě hliníku následuje tenká vrstva plastu, která slouží jako ochrana před poškrábáním. Poslední vrstvou je pak sítotisk, jehož úkolem je odlišení

---

<sup>1</sup> Pit – anglicky prohlubeň, Land – anglicky plocha, Jedná se o reliéf díky kterému se na optických nosičích mění intenzita odraženého světla



jednotlivých nosičů a jejich popisu. Citlivější na mechanické poškození je navzdory obecně rozšířeného názoru vrchní potištěná strana. Proto je vhodné popisovat CD a DVD nosiče nejlépe fixem, aby se neporušila odrazová vrstva.

Samotné čtení disku probíhá tak, že po spirálovité stopě se pohybuje laserový paprsek, který se podle typu povrchu odráží do fotobuňky, jež vytváří elektrické impulzy. Tyto impulzy vznikají změnou odrazu při přechodu land – pit. Při dopadu laserového paprsku na pit dojde k plnému odrazu a paprsek odrážený od landu se silně rozptýlí. Takový přechod z pitu na land se interpretuje jako jednička a určitá část bez změny jako 0. Vzhledem k technice záznamu nul a jedniček na disky CD a DVD, kde není možné, aby byly dvě jedničky vedle sebe, používá se k zápisu na CD 14bitové kódování a na DVD 16bitové kódování. Jejich převod na 8bit je označován jako 8/14 a 8/16 modulace.

Jak uvádí ve své publikaci Dembowski druhy CD a DVD nosičů se liší i podle možnosti jejich použití. Jednotlivé formy jsou i v drobnostech konstrukčně odlišné od výše popsaného modelu, který platí pro disky CD rom a DVD rom neboli disky průmyslově vytvářené s neměnným obsahem dat. Dále rozlišujeme disky na zapisovatelné a prepisovatelné. Zapisovatelné disky slouží k jednorázovému zápisu dat pomocí vypalovací mechaniky. Zásadní rozdíl v konstrukci těchto disků je ten, že obsahují vrstvu organického barviva (například cyanin), do níž je možné vypálit zapisovacím laserem pity a landy. Tento laser má mnohem větší intenzitu, než laser čtecí. Právě díky vrstvě organického barviva je zapisovatelný disk mnohem náchylnější k poškození, například vysokou teplotou. Prepisovatelný disk má ve své struktuře speciální vrstvu, která obsahuje množství kovových prvků (jako jsou například telur, selen a germanium). Zvláštnost této struktury záleží v tom, že je při vystavení teple schopna změnit svou fázi, což znamená, že se dokáže měnit její struktura z krystalické na amorfnní a naopak. Nad touto vrstvou se nachází ještě jedna odrazivá hliníková vrstva. Pro vyvolání fázové změny je nutné aktivovat laser, který je schopen pracovat v režimech s různou intenzitou paprsku. Při zápisu dat se vrstva pro záznam zahřívá bod po bodu na dvě různé teploty. Následujícím ochlazením vzniká krystalická a amorfnní fáze. Krystalická fáze vzniká po zahřátí na nižší teplotu a amorfnní fáze je výsledkem zahřátí na vyšší teplotu. Tento princip přechodu umožňuje prosté prepisování uložených dat bez předchozího vymazání. Samotné přechody fází na disku fungují jako pity a landy na klasických discích. Hliníková vrstva za záznamovou vrstvou odráží paprsek přes krystalické části disku silněji než přes amorfnní části. Vzhledem k slabším odrazům je pro čtení



přepisovatelných disků potřeba citlivější optická soustava, a proto starší mechaniky měly problémy se čtením médií typu RW (přepisovatelné disky). [1, s. 280 - 286]

Některé disky DVD mají také odlišnou stavbu média. Vzhledem k drobnějším záznamovým stopám je možné zapisovat na jednu stranu disku ve dvou vrstvách. Tímto systémem se zvětší kapacita disku ze 4, 7 GB na 8, 5 GB. Navýšení kapacity není dvojnásobné, protože pity a landy ve druhé vrstvě musí být větší kvůli lepší čitelnosti.

### *Paměti typu Flash*

---

Jedny z prvních pamětí flash se využívaly (a dodnes využívají) pro uložení BIOSu v osobních počítačích. Dále se začaly používat v prostředích, která nejsou příliš vhodná pro klasické harddisky tj., příliš prašná, vlhká či s velkými vibracemi. Flash pamětím takové podmínky nevadí, neboť jsou založené na polovodičové technologii. K jejich vymazání či k zapsání dat je potřeba elektrická energie, ale pro uchování již potřeba není.

Paměti flash jsou přímými nástupci elektricky programovatelných pamětí. Zásadní rozdíl a posun v technologii oproti programovatelným pamětím spatřujeme v tom, že na současné flash paměti je možné provádět operace jako zápis nebo vymazání po různě velkých blocích. Dříve se elektricky programovatelné paměti mazaly pouze jako celek. Jednotlivé bloky nabývají rozměry mezi 256 bajty a 128 KB, tudíž není možný přístup k jednotlivým bitům. Pro běžné použití, tím je myšleno ukládání uživatelských dat, se nejčastěji používají bloky o velikosti 512 B. Samotný hardware flash pamětí je uspořádán v několika provedeních, která se liší uspořádáním. Každé z těchto uspořádání se hodí pro jiné účely. Typy NAND a AND umožňují relativně rychlý přístup k zapsaným datům, proto se tato uspořádání používají převážně u paměťových karet. Odlišné typy NOR a DINOR se vyznačují vysokou hustotou a spolehlivostí, proto se využívají hlavně k uložení BIOSu. Samotná technologie flash disků je činí velice odolnými proti mechanickému poškození, nebo vůči magnetickým polím. K počítači se flash disky často připojují přes rozhraní IDE. Protože podporují sadu příkazů ATA, mohou teoreticky plnit funkci standardního pevného disku.

Jedním z nejběžnějších zástupců flash disků jsou paměťové karty, které jsou nejvíce využívány v malých zařízeních, jakými jsou fotoaparáty nebo mobilní telefony. Přestože

všechny typy paměťových karet fungují na stejném principu, mají velké množství vzájemně odlišných rozhraní. Tyto rozdíly vznikly na základě konkurenčního boje výrobců. Nejčastěji používané typy jsou SD, XD a Compact flash. Každá z těchto karet má různý tvar a chceme-li číst data z každého z výše zmíněných typů karet, je třeba počítat s nutností použití čtečky karet, běžně připojovanou přes rozhraní USB. Některá zařízení, především přenosná, bývají opatřena vestavěnými čtečkami karet, nejčastěji pro karty formátu SD a XD, které jsou poměrně malé a čtecí zařízení lze zabudovat do stejného portu. Běžná kapacita těchto karet dosahuje velikosti až 64 GB a s postupem času se na trhu objevují stále větší.

Dalším a asi nejznámějším typem jsou USB flash disky, které mají typ technologie ukládání dat přímo ve svém názvu. Tato zařízení jsou mezi uživateli velmi oblíbená a vyrábějí se v nejrůznějších provedeních (jako přívěšky ke klíčům, nebo jako přehrávač MP3). Jejich hlavní výhodou tkví v jejich fyzické velikosti, přenositelnosti a v neposlední řadě též kapacitě. Běžně jsou USB flash disky k dostání ve velikostech od 128 MB (hlavně starší typy) až po 128 GB. Hlavní negativní stránkou používání těchto největších disků je jejich cena. Nejběžnější velikosti s jakými se běžně setkáváme, jsou od 1 GB do 8 GB. Přímou z názvu těchto médií je jasné, že se k počítači připojují přímo přes rozhraní USB. Současným standardem je rozhraní USB 2.0. V operačním systému Windows se po připojení USB flash disk zobrazuje jako vyměnitelná disková jednotka. Systémy Windows XP, Vista a 7 většinu disků bez problému rozezná, to znamená, že jsou připravené k použití během velmi krátkého času. Starší systémy (například Windows 98) vyžadují instalaci ovládacího softwaru z externího umístění. Proto u většiny starých USB flash disků bylo v prodejním balení i mini CD s ovladači k danému zařízení.

I v nových verzích Windows se nezřídka stane, že systém připojené USB zařízení nerozpozná. Je to většinou dáno nekorektním odhlášením či odebráním hardwaru ze systému bez softwarového ukončení. Je tedy záhodno disky vždy nejdříve odebrat softwarově. Zamezí se tím chybám při příštím připojení k počítači a také se zabrání kolapsu uložených dat, která se mohou poškodit, je-li práce s nimi nekorektně přerušena.

## Poškození dat

---

Poškozená data lze definovat několika způsoby. Obecně lze však říci, že data, ke kterým se nelze dostat jsou svým způsobem poškozená či ztracená. Asi nejčastější poškození dat, s nímž jsem se kdy setkala, bylo způsobeno hardwarovou závadou. Dalším častým způsobem poškození je uživatelská chyba – ta se může projevit několika způsoby. Soubor může mít například špatně přepsanou příponu, nebo uživatel může zapomenout heslo, které chrání přístup k souboru. Další z možností je softwarové poškození způsobené například viry.

## *Poškození hardware*

---

Hardwarová součástka, která má největší vliv na poškození dat, je nepochybně úložné médium. Nejčastěji poškozovaná média jsou pevné disky, optické disky a diskety. Médium s nejnižší pravděpodobností poškození jsou flash disky.

Poškodit pevný disk není velký problém. Hovoříme-li o poškození pevného disku vnějšími vlivy, stačí působení příliš vysoké teploty, pád z poměrně malé výšky, magnetické pole nebo výboj statické elektřiny. Další poškození způsobuje prosté používání, na magnetické vrstvě pro zápis se časem projeví opotřebení. Časem se tak postupně zmenšuje kapacita disku, jelikož se stále nové sektory zapisují do chybové tabulky. Vysoká teplota z důvodu nedostatečného chlazení může zapříčinit zadření disku způsobené teplotní roztažností materiálu ploten. Může se tak stát, že se plotna opře buď o obal disku, nebo o čtecí hlavu. Takový disk je většinou nenávratně poškozen, ale stále existuje způsob, jak jednorázově takový disk rozběhnout. Prakticky vyzkoušený způsob spočívá v umístění disku do antistatického obalu a následně jeho vložení do mrazničky na několik minut. Silné podchlazení může způsobit, že se diskové plotny vrátí do původní pozice a disk tím pádem půjde rozběhnout alespoň pro účel rychlého vykopírování dat. Bohužel, ne všechna data jdou takto zachránit. Pokud dojde k zaseknutí disku o čtecí hlavu, budou oblasti, kde došlo k fyzickému kontaktu nevratně poškozené. Další fyzická poškození naneštěstí takto obejít nelze, např. při pádu se diskové plotny mohou rozlomit a z takto poničených ploten již není možné data jakýmkoliv způsobem znovu získat. K rozlomení může dojít i při závadě elektromotoru, jenž roztáčí diskové plotny. Při příliš vysoké rychlosti se diskové plotny mohou roztrhnout. Magnetické pole či výboj statické energie může pevný disk nezvratně

vymazat. Proto je nutné dbát při fyzickém zacházení s pevným diskem na vybití statické elektřiny o kostru šasi počítače.

Poškodit data na disketě je, bohužel, velmi snadné. K poškození a následné ztrátě dat může dojít pomocí velice slabého magnetu. Další fyzické poškození může vzniknout pouhým dotykem prstu na kotouč floppy, usazením sebemenší částičky prachu, nebo mastným otisk znemožňujícím čtecí hlavě přečíst uložená data.

Poškození optického média vždy neznamenaá úplnou ztrátu dat. Nejčastější poškození těchto médií tvoří škrábance povrchu disku. Drobné poškrábání spodní průhledné části disku nemusí vůbec narušit možnost čtení uložených dat. V těchto případech velmi závisí na velikosti, četnosti a hloubce škrábanců. Hlubší škrábanec, jasně viditelný, může zabránit čtecímu paprsku k dosažení zapsané vrstvy. Horší poškození optického média nastává v okamžiku poškození vrchní odrazivé vrstvy. Takto poškozený disk je, bohužel, již úplně nečitelný.

Fyzické poškození flash disků se liší podle typu disku se kterým pracujeme. Drobné paměťové karty se dají silou rozlomit či se jim častým používáním setrou kontakty. U větších paměťových karet, konkrétně u typu compact flash je nebezpečí v tenkých kontaktech na čtečkách těchto karet. Tenké pinové kontakty se mohou ohnout nebo utrhnout, což ve většině případů sice zničí pouze čtečku, ale může se i stát že utržený pin zůstane zablokován v kartě, která je tímto dále nepoužitelná. USB flash disk v jistých případech lze považovat za téměř nezničitelný při běžném používání. Největším rizikem pro USB flash disk je příliš zvědavý uživatel, který se disk pokouší záměrně poškodit. Druhým největším rizikem je nejslabší místo disku a to konektor USB. U některých typů disků, především s vysouvacím konektorem, hrozí ulomení konektoru od zbytku zařízení. Další riziko je přenášet USB flash disk bez krytky konektoru USB, protože pokud se konektor ucpe či silně zašpiní, nepůjde zasunout do zdířky a přečíst na něm uložená data. Přes všechna tato rizika je většina případů poškozených dat na flash discích je způsobena chybou softwaru nebo chybným zákrokem uživatele. Například hardwarové odpojení disku bez softwarově ukončené funkce může způsobit vymazání nebo nedostupnost některých oblastí disku.

Při vyslovení slov „softwarové poškození dat“ si většina lidí představí počítačový virus. V zásadě je pravda, že většina softwarových poškození dat je opravdu způsobena virem. Ale jsou i jiné způsoby, jak lze softwarově data poškodit. Jedním z nich je i například zapomenuté heslo; soubor tedy není poškozen, ale jeho obsah je pro uživatele tak jako tak nedostupný a musí se podstoupit mnoho kroků k jeho otevření. Všechny pokusy mnohdy končí, žel Bohu, nezdarem. Další softwarová poškození mohou vzniknout například chybami v komprimovaných archivech, nebo ztrátou kontrolních souborů archivů. Další možná rizika mohou skýtat chyby okolního softwaru, například v operačním systému. Při celkovém kolapsu systému se může stát, že data na pevném disku nejsou dostupná.

Jednou z největších hrozeb je škodlivý software, například ve formě počítačových virů. Jak uvádí ve své publikaci Doseděl podstatou viru je šíření mezi počítačovými stanicemi. První virus byl vytvořen roku 1988 studentem americké univerzity Robertem Tappan Morrisem. Původní účel tohoto „červa“<sup>1</sup> bylo zjištění možnosti šíření souborů v internetu. Červ ale obsahoval chyby ve zdrojovém kódu, a tak při svém šíření poškodil řadu systémů a způsobil kolaps většiny tehdejšího internetu. Od té doby se mnohé změnilo. Viry se začaly vytvářet záměrně tak, aby poškodily obsah počítače. Po rozšíření virových hrozeb se vyvinulo úsilí směřující k vývoji antivirových softwarů. Postupným pokrokem v této oblasti výzkumu se viry i antivirové metody začaly měnit. Viry se programují tak, aby nebyly detekovány antivirovými programy. Antivirové programy naproti tomu neustále rozšiřují své databáze, aby byly schopny detekovat nejnovější viry. [3, s.127, 128]

Samotné viry můžeme rozdělit do několika základních skupin. Jako první jsou viry, šířící se pomocí boot sektoru<sup>2</sup> disku. Takový virus přepíše boot sektor, oblast disku ze které se startuje operační systém, takže je prvním softwarem, který se zavádí. Poté spustí samotný operační systém, ale s drobnými rozdíly – například zabrání spuštění residenčních štítů antivirového softwaru. Dále se šíří pomocí disket zapomenutých v mechanice. Díky postavení disketové mechaniky v hierarchii systému se virus může rozšířit do dalších neinfikovaných počítačů. Protože jsou diskety na ústupu a při nouzovém spouštění systému se používají disky CD, tak se tyto viry vyskytují stále méně.

---

<sup>1</sup> Program, který se šíří internetem bez vědomí uživatelů

<sup>2</sup> Zaváděcí sektor disku – místo kde je uložen operační systém. Tato část disku je aktivována z BIOSu hned po spuštění.

Další typy virů se šíří pomocí různých souborů. Takto šířené viry jsou jedny z nejběžnějších. Často jsou připojené ke spustitelným souborům, například s příponou \*.exe nebo k obrazovým souborům například s příponou \*.JPEG. Odlišným virem, který se šíří pomocí jiných souborů jsou makroviry. Ty se šíří hlavně díky implementaci programovacího jazyka Visual Basic do aplikací kancelářského balíku firmy Microsoft.

Viry, jež nepotřebují ke svému šíření podpůrný soubor, jsou takzvaní červi. Jedná se o samostatný spustitelný program. Takto zavirované soubory se šíří hlavně pomocí emailových klientů (Microsoft Outlook, Lotus notes, Mozilla Thunderbird aj.) nebo klientů instant messaging (například ICQ, QIP, Skype a další). Tyto soubory jsou koncipovány tak, aby byl obsah zavirovaného souboru přitažlivý pro většinu uživatelů. Proto se většina těchto virů nazývá podle slavných osobností nebo se maskují jako příjemné zprávy (například virus šířící se pod názvem „Love Letter“). Častá podoba červů se skrývá v podobě souboru s dvojitou příponou. Například Obrázek „.jpg. vbs“. Standardně se objeví jen první přípona a uživatel nechtěně virus spustí.

Podle Doseděla samotný boj proti virům ztěžují programátorské praktiky specifické pro tuto oblast. Základním účelem virů je jejich šíření. Aby se tomuto účelu nedalo tak snadno zabránit jsou viry naprogramovány většinou tak, aby se postupně měnily a ztížily tak svou detekci. Souhrnně se technologie viru nazývají „stealth“, což v překladu znamená neviditelnost. Pod tento název lze zařadit tyto způsoby přizpůsobování: Přepojení služeb operačního systému, aby se skryla změna velikosti souboru, k němuž se virus přikopíroval. Napadání součástí antivirových programů, vypínání rezistenčních štítů, smazání svého kódu z antivirové databáze. Takové chování se označuje jako agresivní. Mutační viry naopak při každém zkopírování změni stavbu své signatury. Tyto viry překombinují hluché sekvence svého kódu tak, aby nebyly hned rozpoznány. A jako poslední typ skrývání lze označit šifrování těla viru tak, aby nebyl rozpoznatelný například podle informačních hlášek, které se zobrazují uživateli. [3, s. 135]

Účinnou ochranu proti virům nabízejí především včas aktualizované antivirové systémy. V současné době lze na internetu najít dostatek solidních antivirových programů poskytovaných zdarma, takže není problém svůj počítač chránit. Antivirové programy používají tři základní metody virové detekce. První je vyhledávání virů podle signatur. Signatura je unikátní řetězec

vlastní jednotlivým virům. Antivirový program pak spouští kontrolu souborů, při níž se signatury jednotlivých spustitelných souborů porovnávají s databází virových signatur. Výhodou této metody je, že spolu s databází se instalují i pokyny, jak většinu zavirovaných programů léčit. Tato léčba probíhá tak, že podle instrukcí se odstraní a zničí tělo viru ze souboru a přepíše se hlavička, která umožňovala jeho spuštění. Další metodou je heuristická analýza. Tato metoda se zakládá na přezkoumávání činnosti programů. Ne všechny činnosti vykonávané programem jsou obvyklé, například zápis do boot sektoru disku. Analýza probíhá přezkoumáváním jednotlivých řádků programů, přičemž jde o zdoluhavý proces, jehož výstupem jsou často chybné nálezy, ale přesto je to jednou z mála možností jak objevit neznámý virus. Nevýhodou je nemožnost léčení viru, jelikož není znám proces změny souboru. Častým výstupem heuristické analýzy je odeslání dat do společnosti vyvíjející daný antivirový software. Vzhledem k nárokům heuristické analýzy na hardware a rychlost počítače je často kombinována s metodou vyhledávání virů na základě signatur. Jako poslední zde uvádím méně často používanou metodou vyhledávání virů, a to CRC Check neboli kontrola kontrolních součtů. U napadnutelných souborů je vypočítán kontrolní součet (CRC), při testování je každý soubor znovu přepočítán a při změně velikosti je vyhlášen poplach. Tato analýza nelze použít na často upravované typy souborů například na textové dokumenty.

Další softwarové ohrožení nejsou klasické viry, i když jsou tak uživateli často nazývány. Jedná se o tzv. „trojské koně“ a „spyware“. Typickým znakem tohoto „malwaru“ (škodlivého softwaru) je, že nenapadají jiné soubory. Jsou většinou součástí nějakého programu. Pod během programu, který je často uživatelem dobrovolně nainstalován, provádí škodlivou činnost. Spyware nejčastěji pasivně sleduje aktivitu uživatele během práce na počítači a získaná data odesílá svému tvůrci. Takto získaná data většinou slouží k zacílení reklamy. Sledují se především otevírané webové stránky a zadávané emailové adresy buď přes webová rozhraní poštovních serverů, nebo v poštovních programech jako jsou například Microsoft Office nebo Mozilla Thunderbird. Pokud uživatel nemá nainstalovanou antispymwarovou ochranu, která bývá součástí některých antivirových programů, bývá první známkou nakažení spywarem zvýšený počet spamových emailů. Druhým nejčastějším malwarem jsou trojské koně. Tento typ škodlivého software se projevuje zvýšenou konektivitou počítače na vzdálené servery. Úkolem trojských koní je odesílat svému tvůrci například hesla vyplněná uživatelem. Tímto způsobem je pak možné proniknout například do emailové schránky uživatele bez jeho vědomí a využít jí kupř. k šíření protizákonných materiálů.



Softwarová chyba nemusí znamenat jen virus či jiný malware, ale i například chyby při komprimaci souborů. Takové chyby se nejčastěji stávají při komprimaci velkých souborů nebo při nouzové komprimaci dat pro přesunutí na záložní datové médium. V takových případech je občas možné data zachránit, bohužel, v případě velkých archivů může nastat částečná ztráta dat. Další softwarové chyby mohou vzniknout při chybě systému, například při nepředpokládaném vypnutí pracovní stanice. V takovém případě se může poškodit tabulka FAT, která uchovává data o umístění volných clusterů na plochách disku.

Jako poslední softwarové ohrožení je činnost samotného uživatele. Uživatel chce chránit svá data, a tak si vytvoří zaheslovaný archiv nebo textový dokument. Problém může nastat v okamžiku, kdy heslo zapomene, nebo je soubor přenesen do jiného prostředí například s klávesnicí nastavenou pro jiný jazyk. Proti takovému ohrožení je několik možností jak data ochránit. Jednou z nich je uvážení, zda je skutečně třeba opatřovat daný soubor heslem. Další je mít systém hesel, v nichž se nevyskytují znaky typické pro jedno jazykové rozložení klávesnice (písmena s háčky a čárky, neobvyklé znaky jako jsou podtržítka, znak pro procenta a podobné). Poslední možností je software pro dešifrování souborů. Tento proces je ovšem časově velice náročný a bohužel většina softwarů pro tyto účely jsou zpoplatněné a většinou i dosti drahé. Sama jsem několik takových programů vyzkoušela bez valného úspěchu. Hesla z cizích souborů stažených z internetu se mi nikdy nepodařilo prolomit a hesla mnou vytvořená pro účel testování takového softwaru se dešifrovala i několik dnů i za předpokladu, že jsem měla k dispozici délku hesla i použitou znakovou sadu. Dalším ztrátám ze strany uživatele může dojít nepozorností práce s daty. Není výjimkou, že uživatel omylem smaže data z pevného disku či jiného vymazatelného úložiště. V takových případech lze po jistou dobu data zachránit. Méně častá, ale pravděpodobná varianta je celkové naformátování disku.

Nejčastější poškození dat je způsobeno samotnými uživateli. Během praxe jsem se setkala s častou žádostí o restaurování vymazaných dat. Další frekventovanou závadou jsou chyby pevných disků; tento fakt je dán tím, že pevný disk je nejčastějším datovým nosičem. S poškozením dat viry jsem se během praxe téměř nesetkala. Virus většinou způsobil nemožnost práce s počítačem, nikoliv ztrátu dat, ale přesto existuje reálná hrozba virů, které mohou zformátovat harddisk nebo způsobit nechtěné změny v textových souborech.



## **Způsob pro znovuzískání ztracených dat**

---

Nejfrekventovanějším problémem, se kterým se setkává IT opravář jsou ztracená data z harddisků. Jednoduché vysvětlení spočívá ve skutečnosti, že harddisk je nejčastěji používané médium pro práci s daty. Osobně si neumím představit osobní počítač nebo notebook bez pevného disku. Existují sice kombinované disky, které používají jak technologii pevného disku, tak technologii flash, ale jejich rozšíření vzhledem k jejich ceně je minimální. Další způsob ztráty dat je často způsoben nejrůznějšími viry, ale v principu většina z nich funguje na bázi klasického smazání dat z disku. V horším případě obsahuje virus kód, který přepíše uvolněné clustery disku. Tehdy dochází k trvalé ztrátě dat z disku.

Operační systém data na disku ukládá do clusterů, které jsou uspořádány do stop a cylindrů. Pro práci s clustery se používá logická tabulka (FAT, NFTS), která určuje, jaký soubor je v jakém clusteru zapsán a jaká je jeho finální velikost. V zásadě se v logické tabulce objevují tři hlavní druhy záznamů, a to: volný cluster, obsazený cluster a poškozený cluster. Při mazání souboru se nevymaže přímo místo na disku, pouze se změní hodnota v logické tabulce přiřazená k danému clusteru. Dokud takto uvolněný cluster není přepsán jinými daty, je možné obnovit jeho předchozí obsah. Proto existují programy na přepsání volného místa na disku, čímž znemožňují neoprávněné přečtení vymazaných dat. Běžně systém zapisuje data do clusterů řazených za sebou. Tudíž, představíme-li si model disku v podobě povrchu jediné plotny, budou data postupně zaplňovat povrch plotny od středových stop k okrajovým. Uvolněná místa se začnou přepisovat v okamžiku, kdy na konci disku již nezbyvá dostatek místa k uložení požadovaných dat. Z toho vyplývá, že je snazší obnovit smazané soubory na poměrně velkém a volném disku, než na disku, který nabízí malé množství volné kapacity.

Při naformátování harddisku dojde k vyčištění logické tabulky, která zapisuje polohu jednotlivých dat v clusterech disku. V případě, že se po naformátování s diskem dále datově nemanipuluje, existuje reálná možnost, že většina dat bude ještě zachráněna. K účelu získání dat z naformátovaného disku se používá poměrně drahý software (například Symantec Northon Ghost). Proto pro běžného uživatele je nejlepším řešením takto poškozený disk svěřit odborníkům, kteří vlastní nutný software k obnovení disku a především mají zkušenosti, jak takovou obnovu provést s nejmenším rizikem definitivní ztráty dat. Při amatérském obnovení disku může dojít k závažným chybám, například kombinací k sobě nepatřících částí souborů.

V případě vymazání některých souborů je přímo v systému Windows integrována první záchranná síť ve formě programu Recycle bin (Koš). Koš umožňuje uživateli odstranit soubor, tudíž si zdánlivě uvolnit místo na disku. Při odstraňování extrémně velkých souborů (například film v HD kvalitě) se zobrazí hláška, že soubor je příliš velký pro přesunutí do koše spolu s dotazem, zda se má soubor přímo odstranit. Koš má totiž na disku vymezené místo pro odstraněné soubory a pokud soubor tuto velikost přesáhne, musí být odstraněn přímo z logické tabulky.

Soubory úplně vymazané buď vysypáním z koše, nebo příkazem SHIFT + DELETE nemusí být ztraceny, pokud disk není ještě přeplněný. K jejich rekonstrukci existuje množství softwarů, které fungují na principu obnovení předchozího stavu logické tabulky. Většinou je nutné znát, jaký typ souboru byl vymazán a o zbytek se již postará samotný obnovovací software.

Pro získání dat z poškozeného optického nosiče existují opravné substance, které mohou odstranit poškrábání spodní transparentní části disku. Pokud škrábance nezasáhly nosnou vrstvu s pity a landy, je oprava takového nosiče téměř bezriziková pro uložená data. V případě hlubokého poškození transparentní vrstvy, kdy jsou zasaženy pity a landy, tyto substance fungují pouze pro ulehčení přečtení zbytku disku. Data uložená v místech fyzického poškození jsou ztracena. Hovoříme-li o extrému, při poškození svrchní odrazivé vrstvy je třeba konstatovat, že možnost obnovy ztracených dat již v podstatě byla vyčerpána.

Existuje velké množství způsobů pro záchranu ztracených dat, ale žádný z nich není stoprocentně účinný nebo bezchybný. Pro uchování důležitých uživatelských dat je nejbezpečnějším prostředkem vytváření záloh souborů.

## **Zálohování**

---

V předchozích kapitolách jsem popsala jakým způsobem lze o data přijít i několik možností jak je získat zpět. Pro svou práci jsem vybrala jako nejspolehlivější způsob obnovy dat zálohování. V této části bude popsáno testování dvou uživatelsky nejlépe hodnocených programů pro zálohování ze serveru [www.stahuj.cz](http://www.stahuj.cz) a zálohovací systém integrovaný přímo v systém Windows. Hodnocení na serveru [www.stahuj.cz](http://www.stahuj.cz) vytvářené uživateli má podobu jedné až pěti hvězdiček u každého programu. Pro bližší orientaci jsou u programů poskytnuty takzvané mini recenze, kde uživatelé krátce hodnotí klady a zápory programu. Jak Pro možnost objektivního srovnání zde bude také popsáno kopírování souborů na externí úložiště.

Pro testování jsem použila netbook DELL (Inspiron Mini 1010) a externí harddisk Western Digital o kapacitě 500 GB. Základní hardwarové parametry netbooku jsou dány procesorem Intel Atom o frekvenci 1.60 GHz, paměť RAM o velikosti 1 GB rozšířenou pomocí funkce ready boost na velikost 4 GB a pevným diskem o kapacitě 150 GB. Operační systém je tvořen 32bitovou verzí Windows 7 Professional s nainstalovanou standardní sadou Microsoft office.

### *Volba média*

---

Výběr datového média je závislý především na dalším použití uložených dat a na vztahu ceny a trvanlivosti média. Pro zálohy uživatelských dat, které slouží pouze k obnovení dat nebo přenesení na další počítač uživatele jsou vhodná média, která nelze snadno poškodit. Případně je lze snadno ochránit před poškozením.

### *Kopírování souborů*

---

Běžné kopírování dat na externí pevný disk bylo provedeno pomocí programu Total Commander. Tento software je volně šiřitelný, ale s licencí shareware, proto při každém spuštění žádá po uživateli zaplatit licenci. Po zaplacení licence zmizí okno, kde je nutné odkliknout správné číslo pro přístup do programu. Jiným způsobem není používání programu Total Commander omezeno.

Celkový objem dat má velikost 13,1 GB rozdělených mezi 3 188 souborů. Jako typické zástupce dat jsem zvolila soubory řádově ve velikosti maximálně desítek MB. Největší soubor celé zálohy má 91MB.

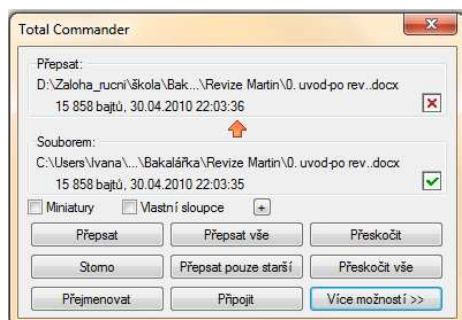


Obr. 1 - Licence programu Total Commander

Celkový čas potřebný na zálohu byl 35 minut včetně výběru souborů zálohy a vytvoření jednoduché datové struktury. Výsledná záloha je velikostně 1:1 k originálním souborům.

Výsledná podoba zálohy čistě záleží na uživateli. Jednotlivé soubory jsou po připojení externího disku k počítači čitelná stejným způsobem jako před provedením zálohy.

Při přidávání souborů zálohy je na uživateli zda zvolí kopírování jednotlivých nových či změněných souborů do složek či zda zkopíruje celou adresářovou strukturu. Při druhé verzi postupu existuje nebezpečí duplikovaných stejných souborů v různých složkách. Program Total Commander analyzuje při kopírování souboru zda ve výsledném umístění již existuje v dané složce soubor stejného názvu. V případě shody názvu souborů ve zdrojové i cílové složce nabídne uživateli jak se zachovat. Zda má soubor přepsat, přepsat starší verzi nebo úplně přeskočit.



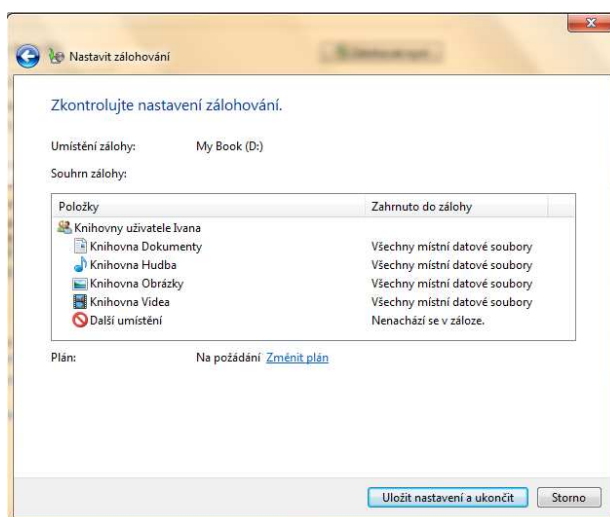
Obr. 2 - Total Commander - přepis souboru

Pro ověření funkce přidání nových souborů k záloze jsem do jednoho adresáře přidala složku souborů o velikosti 147MB. Přidání této složky k ručně vytvořené záloze pomocí programu Total Commander trvalo méně než půl minuty.

### *Windows zálohování*

Jako první zálohovací software jsem využila možnost, kterou nabízí přímo operační systém. Jedná se o funkci zálohování a obnovování. Program se nabídne při prvním spuštění nově nainstalovaného počítače. Zde má uživatel možnost nastavit si plán pravidelného zálohování. Uživatel má dvě základní možnosti vytváření záloh pomocí Windows.

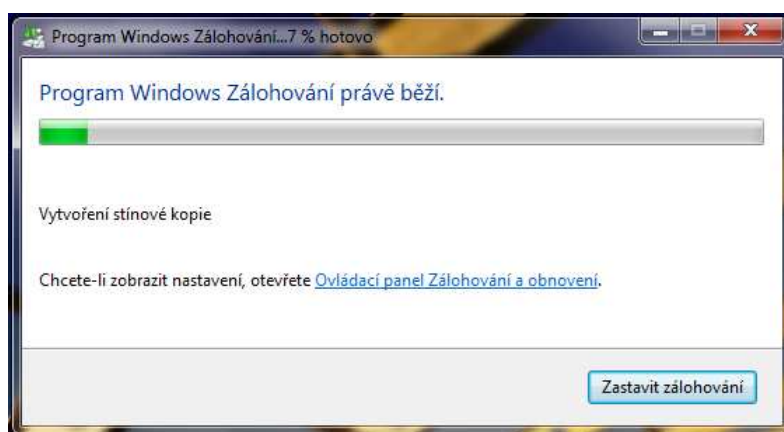
První je zcela automatická funkce systému, kdy se zálohují veškerá data i nastavení operačního systému. Nevýhodou automatické zálohy je především její velikost. Při kopírování se zkopírují pouze soubory, které uživatel chce chránit před ztracením. Při zálohování malého množství dat je automatická záloha Windows mnohem větší než samotná data. Druhou největší chybou tohoto systému je v okamžiku, kdy chce uživatel se svými daty migrovat na jiný počítač, tj. s odlišným složením hardware i jinou verzí operačního systému. V takovém případě je automatické přenesení uložených souborů nemožné a uživatel je nucen z vytvořených archivů svá data vykopírovat ručně. Tyto zkušenosti se zálohovacím systémem Windows mě přiměly k testování druhé možnosti jež program nabízí.



Obr. 3 - Výběr knihoven zálohy Windows

Manuální zálohování umožňuje uživateli do jisté míry ovlivnit jaká data budou zálohována. Bohužel není možnost výběru jednotlivých složek či adresářových stromů. Nový operační systém Windows 7 nabízí pouze možnost označit knihovny, ve kterých se nachází soubory které chce uživatel zálohovat. V tomto testovacím případě jsem zvolila čtyři základní knihovny, kam se uživatelská data ukládají. Abych zbytečně neprodlužovala čas nutný pro zálohu nezvolila jsem možnost vytvoření bitové kopie systému, která slouží k obnovení nastavení uživatelského rozhraní Windows.

Testovací balík dat je stejný jako u manuálního zálohování tudíž má celkovou velikost 13,1GB. Konečná velikost zálohy je stejná jako objem zálohovaných dat v předchozím případě. Celkový čas nutný pro provedení zálohy je 51 minut.



Obr. 4 - Průběh zálohování ve Windows

Zálohovaná data jsou komprimovaná metodou zip. Stejnou velikost záložních a zálohovaných dat lze vysvětlit tím, že k záloze jsou přidány soubory aplikací, které se ukládají do uživatelských knihoven. Struktura zálohy je soubor 77 zipových souborů ve velikostech od 99 MB do 199 MB. Vyhledání pouze některých dat je časově velmi náročné, protože pro uživatele nemá záloha na první pohled žádný systém. Pro obnovení dat je v záloze obsažen katalogový soubor, který po spuštění umožní obnovovacímu programu zápis dat do správných knihoven a složek.

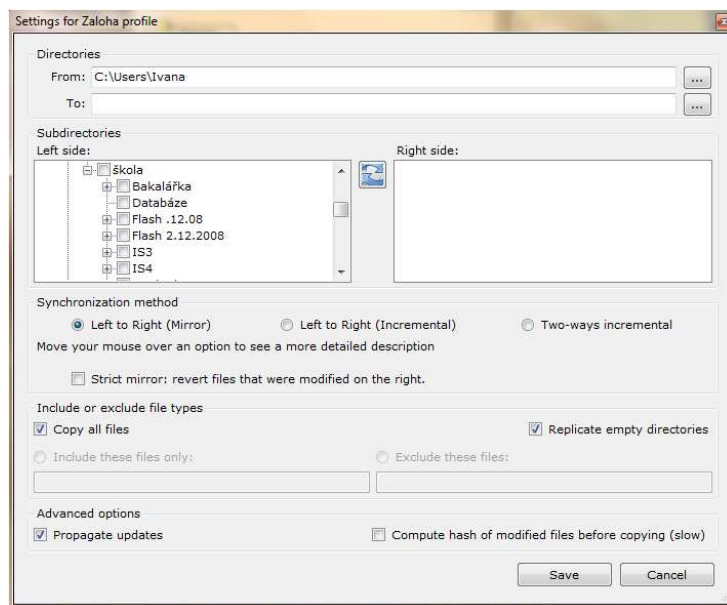
Přidání souborů o velikosti 147 MB k záloze proběhlo poměrně rychle v čase 2 minut. K záložním složkám přibyla nová složka s podadresáři a soubory komprimovanými metodou zip, kde se nacházela pouze nově přidaná data.

## Create synchronicity

Tento program je vydaný jako freewareová licence od autora SourceForge.net. Pro test byla použita verze 2.1.0.0. Krátký popis ze stránek [www.stahuj.cz](http://www.stahuj.cz) je následující [4] "Systémově nenáročná, plně přenosná, open source aplikace navržená za účelem synchronizace a zálohování vámi zvolených dat. Program je velice dobře hodnocen samotnými uživateli, kteří s ním pracují, a nabídnout vám může tyto nástroje:

- plnohodnotná volba dat, která chcete synchronizovat,
- používá tři metody synchronizace (Mirror, One-way incremental, Two-ways incremental),
- hashing souborů,
- podpora zobrazení obsahu souborů,
- podpora více uživatelských profilů,
- možnost přenosu aplikace bez nutnosti reinstalace,
- podpora příkazové řádky."

Program Create synchronicity je freewareový software který je kompletně v angličtině. Při prvním spuštění na počítači s operačním systémem Windows7 je nutné provést základní nastavení aplikace a spouštět ji jako správce.

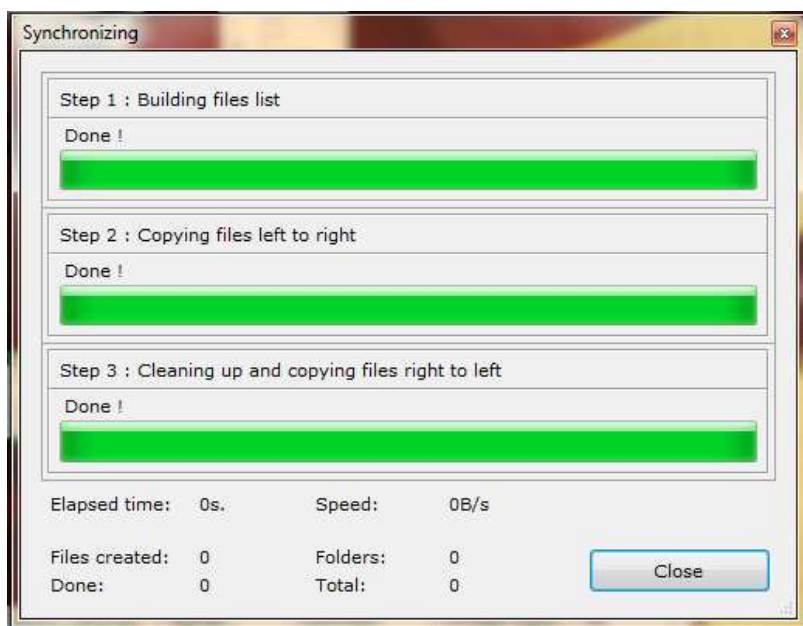


Obr. 5 - Vytvoření profilu v Create Synchronicity



Po spuštění se na obrazovce objeví jednoduchý formulář s nabídkou vytvoření profilu. Po zadání jména profilu se objeví tabulka s nastaveními. Zde je možné nastavit nejen adresáře které se budou zálohovat ale i způsob vytváření záloh. Při zvýraznění jednotlivých profilů záloh se v dolní části formuláře objeví krátký popis zvoleného profilu ve kterém je uveden především název profilu, použitá metoda zálohování a odkaz na hlavní zdrojový a cílový adresář. Create synchronicity používá tři metody synchronizace.

První metoda Mirror<sup>1</sup> v záloze zrcadlí veškeré změny zdrojových dat. To znamená že při vytváření nové zálohy se projeví veškeré změny včetně vymazání některých souborů či adresářů v nastavené struktuře. Metoda One-Way Incremental<sup>2</sup> zálohuje data tak, že k záloze pouze přidává změněné soubory a složky. V záloze se tak nemazou data vymazaná v originálním umístění. Třetí metoda Two-Ways Incremental<sup>3</sup> přidává jak k záloze tak ke zdroji chybějící data, to znamená že vymazaná data v originálu budou při provedení zálohy zkopírována zpět. Při volbě metody je velmi nápomocná funkce rychlé nápovědy, která zobrazí vysvětlení k položce při najetí na její název kurzorem myši.



Obr. 6 - Create Synchronicity, průběh zálohování

<sup>1</sup> Anglicky zrcadlo

<sup>2</sup> Anglicky jednostranně přírůstkový

<sup>3</sup> Anglicky oboustranně přírůstkový



Celková záloha má velikost 13,1 GB a je provedena bez komprese. Samotné kopírování dat trvalo 27 minut. Vytvoření profilu trvalo zhruba dvě minuty takže celkový čas nutný pro zálohu pomocí Create synchronicity je 29 minut. V adresářové struktuře jsou data přehledně uložena velmi podobně jako na zdrojovém disku.

Přidání zálohy o velikosti 147 MB proběhlo bez jakýchkoliv problémů. Za celkový čas 46 vteřin.

Obnovení dat ze zálohy provedené programem Create Synchronicity je možné provést dvěma způsoby a to buď ručně data zkopírovat pomocí souborového manažera, nebo vytvořit zpětný profil, kde bude jako zdroj načteno úložiště se zálohou.

### AASync

---

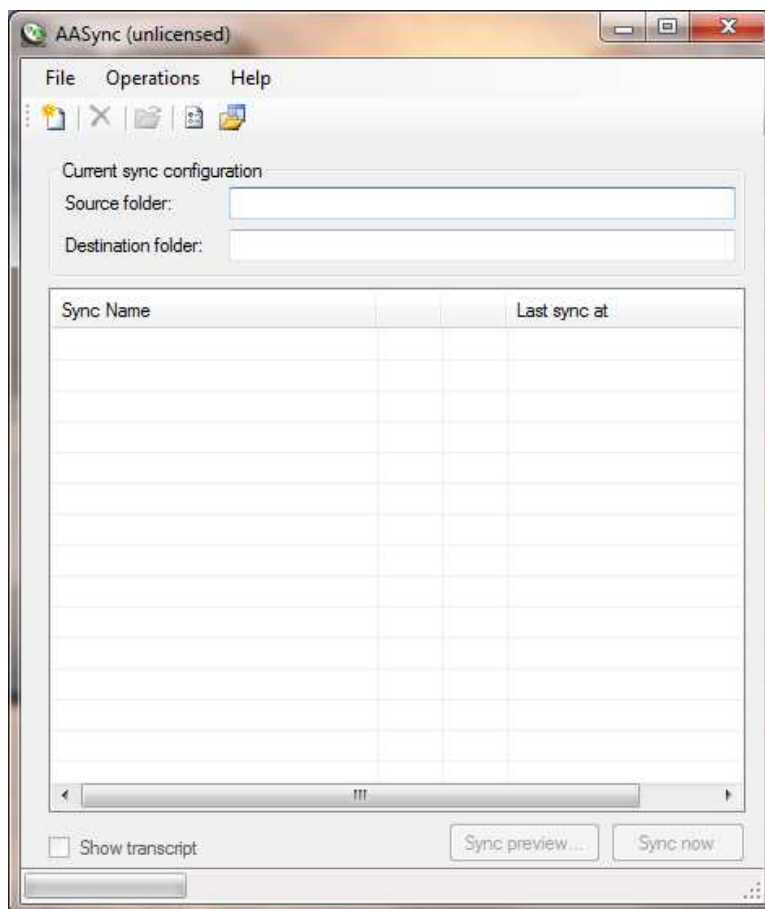
Tento freeware program jehož autorem je AASync je na serveru [www.stahuj.cz](http://www.stahuj.cz) hodnocen uživateli pěti hvězdičkami. Byla použita verze 2.2.1.0. Popis ze stránek [www.stahuj.cz](http://www.stahuj.cz) je následující [5] *"Tento program je universální v tom, že umožňuje jak lokální, tak i vzdálené zálohování a synchronizaci přes FTP nebo FTPS připojení. Pokud je pak takový soubor i nadále zálohován, dokáže program ukládat pouze provedené změny, což rapidně zvyšuje efektivitu práce aplikace."*

#### Nástroje programu:

- *synchronizace adresářů (lokální-lokální, lokální-vzdálený, vzdálený-lokální),*
- *podpora simultánní synchronizace,*
- *možnost ignorování určitých souborů a souborových typů,*
- *ochrana přenosu pomocí ssh šifrování,*
- *různé módy pro synchronizaci,*
- *rychlá záloha pomocí dvoufázového synchronizačního enginu."*

Software AASync je kompletně v anglickém jazyce. Po spuštění se objeví formulář s tabulkou pro různé profily synchronizace. V jednom profilu je možné nastavit pouze jeden adresář s podadreářovou strukturou. Proto je pro zálohu dat bez nadbytečných souborů vytvořených

systemem nutné vytvořit několik profilů pro zálohování. Při tvorbě profilů pro zálohování na místní úložiště jsou možné zvolit mezi pěti režimy.



Obr. 7 - AASync - vytvoření profilu

První režim Automatic postupuje s daty ve dvou krocích. První krok vytvoří zdrojovou databázi (dále DB). Druhý krok pak srovná data ze zdrojové DB s cílovými složkami a poté provede kopírování dat. Druhý režim Source by DB only<sup>1</sup> vytvoří případně obnoví zdrojovou databázi. Třetí režim Source Destination comparison only<sup>2</sup> zkopíruje data ze zdrojové databáze na cílové úložiště. Čtvrtý režim Source DB then source destination comparison<sup>3</sup> provádí předchozí dva režimy po sobě, jedná se o časově náročnější variantu zálohování. Poslední pátý režim je Mirror, který pracuje na stejném principu jako u předchozího softwaru. Celý proces zálohování pomocí AASync byl rozdělen do čtyř profilů, aby se do zálohy nepřidaly žádné nechtěné soubory. Režim zálohování byl nastaven na Automatic. Konečná velikost zálohy má 13,1 GB. Celý proces zálohování včetně vytvoření čtyř zálohovacích

<sup>1</sup> Anglicky pouze zdrojová databáze

<sup>2</sup> Anglicky pouze srovnání cílů

<sup>3</sup> Anglicky Zdrojová DB poté srovnání cílů

profilů a jejich postupného spuštění trval 35 minut. Adresářová struktura kopíruje strukturu zdrojových souborů. Tudíž není problém ruční obnovení souboru ze zálohy.

Přidání souboru o velikosti 147 MB trvalo celkem 3 minuty a proběhlo bez jakýchkoliv problémů.

Obnovení dat ze zálohy je možné provést buď vytvořením zpětných profilů nebo pomocí souborového manažera.

## Závěr

---

V závěru budou zhodnoceny jednotlivé zálohovací programy podle níže uvedených kritérií. Na základě těchto kritérií bude možné také zhodnotit zda byl splněn cíl práce. Pro dosažení úspěchu je potřeba nalézt zálohovací freeware který vytvoří testovací zálohu dat rychleji nebo alespoň za stejný čas jako manuální kopírování souborů.

Hlavní kritéria hodnocení:

- Čas nutný pro zálohu – v tomto údaji je i započítána doba, kterou uživatel musí věnovat spuštění programu a nastavení jednotlivých parametrů
- Velikost záložních souborů a případně typ komprese – nejdůležitější vlastností komprese není úspora místa na záložním médiu, ale snadný přístup k jednotlivým souborům
- Funkčnost aditivního zálohování – přidávání nových souborů k záloze bez opakování zálohy již zapsaných souborů
- Zpracování uživatelského rozhraní – přehlednost menu programu, možnosti nastavení a jazykové možnosti softwaru.

Pro testování zálohovacích programů byl použit balík dat o velikosti 13,1 GB rozdělený do běžně užívaných složek počítače.

Jako první byla použita metoda běžného kopírování dat pomocí souborového manažera (Total Commander). Zde je přehled základních sledovaných vlastností:

- Čas potřebný pro provedení zálohy – 35 minut
- Záložní soubory jsou bez jakékoliv komprese v adresářové struktuře vytvořené uživatelem
- Aditivní zálohování závisí především na znalostech uživatele
- Uživatelské rozhraní a jazyk závisí na použitém softwaru v tomto případě byl použitý SW Total Commander, ale stejnou službu může poskytnout i průzkumník Windows nebo například souborový manažer Salamandr

Ruční zálohování má největší výhodu ve vlastní tvorbě adresářové struktury uživatelem. Usnadní se tím migrace na jiný počítač, kde může být jiná kapacita harddisku, odlišné

požadavky na obsah souborů nebo jiný operační systém. Časová náročnost lze ovlivnit způsobem kopírování, či kopírováním pouze nejn nutnějších souborů v okamžiku časové tísně uživatele a zbytek zálohy provést v jinou dobu.

Druhá použitá metoda bylo zálohování dat pomocí systému integrovaného přímo do Windows. Následuje přehled pozorovaných vlastností:

- Čas potřebný pro provedení zálohy – 51 minuta
- Struktura záložních souborů je pro uživatele komplikovaná vzhledem k množství dat, která uživatel zálohovat nechce a vzhledem ke kompresi dat
- Aditivní zálohování je velmi jednoduché a poměrně rychlé.
- Uživatelské rozhraní je jasné a v jazyce použitého OS.

Zálohování pomocí Windows trvalo ze všech zálohovacích programů nejdéle. Hlavním důvodem zdlouhavého kopírování je nemožnost zvolit pouze určité složky se soubory. Ve výsledku je kopírováno více dat, než je nutné. Díky komprimovanému formátu výsledné zálohy ve velikosti neliší do nekomprimované záloze vytvořené ručním kopírováním.

Další použitou metodou zálohování byl SW Create Synchronicity. Zde je přehled jeho základních parametrů:

- Čas potřebný pro provedení zálohy - 29 minut
- Struktura souborů zálohy kopíruje strukturu vybraných složek ve zdrojovém počítači
- Aditivní záloha proběhla velice rychle díky uloženému zálohovacímu profilu
- Uživatelské rozhraní je velice jednoduché a poměrně dobře zpracované hlavně díky náhledu okamžité nápovědy. Rozhraní je celé v anglickém jazyce.

Software Cerate Synchronicity je uživatelsky velice přívětivý. Možnost vytvoření několika zálohovacích profilů umožňuje snadné přidávání nových souborů do zálohy velmi efektivně. Při rychlostním porovnání byla záloha vytvořena nejrychleji. Rychlost vytvoření zálohy je dána především přehledností menu a rychlým vysvětlivkám k jednotlivým prvkům v uživatelském rozhraní díky kterým nemusí uživatel dohledávat informace v souborech nápovědy nebo na webu.

Jako poslední byl k provedení zálohy použit software AASync s následujícími sledovanými parametry:

- Čas potřebný pro provedení záloh – 35 minut
- Struktura zálohy kopíruje přesně strukturu zvoleného adresáře pro zálohování
- Aditivní záloha proběhla rychle díky vytvořeným profilům a možnosti spustit pouze profil, jehož se nová data týká.
- Uživatelské rozhraní je graficky jednoduše zpracované, ale pro orientaci je nutné znát velice dobře anglický jazyk. I přes jednoduchost zpracování se v nabídkovém menu nový uživatel pohybuje těžce.

Software AASync je software vhodný především pro zkušené uživatele. Vzhledem k většímu množství možných nastavení je práce s programem poněkud zdlouhavá. Přes všechny komplikace s porozuměním si s programem byl výsledný čas 35 minut shodný s manuálním zálohováním. Pro provedení zálohy je nutné vytvořit větší množství profilů protože v jednom profilu nejde vyjmout podadresáře z hlavní složky. Tato nevýhoda při vytváření systému pro zálohování velkého množství dat v nesouvislých umístěních se změní ve výhodu při vytváření dodatečných záloh. Z vytvořených profilů lze vybrat pouze profily se složkami ve kterých se změnily nebo přidaly soubory.

Z výše uvedených faktů je zřejmé, že cíle této práce bylo dosaženo. Nejlepší testovaný software pro zálohování je program Create Synchronicity, který vytvořil zálohu dat o 6 minut rychleji než manuální zálohování. Jeho uživatelské rozhraní je uživatelsky přívětivé. Jednoduchá grafika spolu s nápovědou vestavenou přímo v okně nastavení profilu vyváží pouze anglický jazyk komunikačního rozhraní. Nastavení profilu umožňuje vybírat jednotlivé složky a podsložky datových knihoven tak nedohází k zálohování dat, která uživatel nemá zájem zálohovat.

## Literatura

---

### *Citace*

---

[1] DEMBOWSKI, Claus *Mistrovství v hardware, Nastavení, optimalizace a opravy počítačových komponent* 1. Vyd. Brno: Computer Press, 2009. 701 s. ISBN 978-80-251-2310-2

[2] Wikipedie, otevřená encyklopedie [online]. Wikimedia Foundation, 2001[cit.2010-05-01]. Dostupný z WWW: < <http://cs.wikipedia.org/wiki/Hystereze>>.

[3] DOSEDĚL, Tomáš *Počítačová bezpečnost a ochrana dat* 1. Vyd. Brno: Computer Press, 2004. 183 s. ISBN 80-251-0106-1

[4] Stahuj.cz – Download shareware a freeware [online]. MITON.CZ, 2000 [cit.2010-04-30]. Dostupný z WWW: <[http://www.stahuj.centrum.cz/utility\\_a\\_ostatni/zalohovani/create-synchronicity/](http://www.stahuj.centrum.cz/utility_a_ostatni/zalohovani/create-synchronicity/)>

[5] Stahuj.cz – Download shareware a freeware [online]. MITON.CZ, 2000 [cit.2010-04-30]. Dostupný z WWW: <[http://www.stahuj.centrum.cz/utility\\_a\\_ostatni/zalohovani/aasync/](http://www.stahuj.centrum.cz/utility_a_ostatni/zalohovani/aasync/)>

### *Bibliografie*

---

BISHOP, Matt *Introduction to Computer Security* 1st ed. Boston: Addison-Wesley Professional, 2004 648 s. ISBN 0-321-24744-2

HUNTER, John M. D. *An Information Security Handbook* 1st ed. London: Springer – Verlag, 2001 213 s. ISBN 1-85233-180-1

MINASI, Mark *PC - velký průvodce hardwarem* 1. Vyd. Praha: GRADA Publishing, 1998. 1220 s. ISBN 80-7169-667-6